AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for redirecting data in a network, the network connecting a first gateway and a second gateway, ~~the first gateway comprising a first node and a third node, the second gateway comprising a second node and a fourth node,~~ the method comprising:

transmitting over the network an indication from ~~the~~ a first node in the first gateway to ~~the~~ a second node in the second gateway that ~~the~~ a third node in the first gateway has failed; and

reconfiguring a first data, the first data initially configured to be transmitted over the network between the second node and the third node, to be transmitted over the network between ~~the~~ a fourth node in the second gateway and the first node after the indication has been received by the second node.

2. (Original) The method of claim 1, further comprising configuring the first node and the fourth node to send and receive encrypted data between the first node and the fourth node.

3. (Original) The method of claim 2, further comprising configuring the first node and the fourth node to send and receive the encrypted data between the first node and the fourth node via a first tunnel.

4. (Original) The method of claim 2, further comprising using a security protocol to encrypt the data.

5. (Original) The method of claim 4, wherein the security protocol comprises at least one of Secured Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

6. (Original) The method of claim 1, further comprising configuring the third node and the second node to send and receive encrypted data between the third node and the second node.

7. (Original) The method of claim 6, further comprising configuring the third node and the second node to send and receive the encrypted data between the third node and the second node via a second tunnel.

8. (Original) The method of claim 6, further comprising using a security protocol to encrypt the data.

9. (Original) The method of claim 8, wherein the security protocol comprises at least one of Secured Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

10. (Canceled)

11. (Canceled)

12. (Original) The method of claim 1, wherein transmitting over the network the indication further comprising using Internet Key Exchange (IKE).

13. (Original) The method of claim 1, wherein the network comprises the Internet.

14. (Currently Amended) A system for redirecting data in a network, the network connecting a first gateway and a second gateway~~, the first gateway comprising a first node and a third node, the second gateway comprising a second node and a fourth node,~~ the system comprising:

a component for transmitting over the network an indication from ~~the~~ a first node in the first gateway to ~~the~~ a second node in the second gateway that ~~the~~ a third node in the first gateway has failed; and

a component for reconfiguring a first data, the first data initially configured to be transmitted over the network between the second node and the third node, to be transmitted over the network between ~~the~~ a fourth node in the second gateway and the first node after the indication has been received by the second node.

15. (Original) The system of claim 14, wherein the first node and the fourth node are configured to send and receive encrypted data between the first node and the fourth node.

16. (Original) The system of claim 15, wherein the first node and the fourth node are configured to send and receive encrypted data between the first node and the fourth node via a first tunnel.

17. (Original) The system of claim 15, wherein the data is encrypted with a security protocol.

18. (Original) The system of claim 17, wherein the security protocol comprises at least one of Secured Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

19. (Original) The system of claim 14, wherein the third node and the second node are configured to send and receive encrypted data between the third node and second node.

20. (Original) The system of claim 19, wherein the third node and the second node are configured to send and receive encrypted data between the third node and second node via a second tunnel.

21. (Previously Presented) The system of claim 19, wherein the data is encrypted with a security protocol.

22. (Original) The system of claim 21, wherein the security protocol comprises at least one of Secur(Original) ed Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

23. (Canceled)

24. (Canceled)

25. (Original) The system of claim 14, wherein the component for transmitting over the network the indication is further configured for using Internet Key Exchange (IKE).

26. (Original) The system of claim 14, wherein the network comprises the Internet.

27. (Currently Amended) A computer-readable storage device on which is stored a set of instructions for redirecting data in a network, the network connecting a first gateway and a second gateway~~, the first gateway comprising a first node and a third node, the second gateway comprising a second node and a fourth node,~~ which when executed perform stages comprising:

transmitting over the network an indication from ~~the~~ a first node in the first gateway to ~~the~~ a second node in the second gateway that ~~the~~ a third node in the first gateway has failed; and

reconfiguring a first data, the first data initially configured to be transmitted over the network between the second node and the third node, to be transmitted over the network between ~~the~~ a fourth node in the second gateway and the first node after the indication has been received by the second node.

28. (Previously Presented) The computer-readable storage device of claim 27, further comprising configuring the first node and the fourth node to send and receive encrypted data between the first node and the fourth node.

29. (Previously Presented) The computer-readable storage device of claim 28, further comprising configuring the first node and the fourth node to send and receive the encrypted data between the first node and the fourth node via a first tunnel.

30. (Previously Presented) The computer-readable storage device of claim 28, further comprising using a security protocol to encrypt the encrypted data.

31. (Previously Presented) The computer-readable storage device of claim 30, wherein the security protocol comprises at least one of Secured Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

32. (Previously Presented) The computer-readable storage device of claim 27, further comprising configuring the third node and the second node to send and receive the first data as encrypted data between the third node and second node.

33. (Previously Presented) The computer-readable storage device of claim 32, further comprising configuring the third node and the second node to send and receive the encrypted data between the third node and second node via a second tunnel.

34. (Previously Presented) The computer-readable storage device of claim 32, further comprising using a security protocol to encrypt the encrypted data.

35. (Previously Presented) The computer-readable storage device of claim 34, wherein the security protocol comprises at least one of Secured Socket Layer (SSL), Secure HTTP (SHTTP), Private Communications Technology (PCT), and IP Security (IPSEC).

36. (Canceled)

37. (Canceled)

38. (Previously Presented) The computer-readable storage device of claim 27, wherein transmitting over the network the indication further comprising using Internet Key Exchange (IKE).

39. (Previously Presented) The computer-readable storage device of claim 27, wherein the network comprises the Internet.

40. (New) The method of claim 1, wherein the first data is prioritized based upon message type and network destination.

41. (New) The method of claim 1, wherein the first data is reconfigured so that only the addresses of the first gateway and the second gateway are available to other users of the network.

42. (New) The method of claim 4, wherein the security protocol is configured to only allow the addresses of the first gateway and the second gateway to be available to other users of the network.

43. (New) The method of claim 8, wherein the security protocol is configured to only allow the addresses of the first gateway and the second gateway to be available to other users of the network.

44. (New) The system of claim 14, wherein the first data is prioritized based upon message type and network destination.

45. (New) The system of claim 14, wherein the first data is reconfigured so that only the addresses of the first gateway and the second gateway are available to other users of the network.

46. (New) The system of claim 17, wherein the security protocol allows only the addresses of the first gateway and the second gateway to be available to other users of the network.

47. (New) The system of claim 21, wherein the security protocol allows only the addresses of the first gateway and the second gateway to be available to other users of the network.

48. (New) The computer-readable storage device of claim 27, wherein the first data is prioritized based upon message type and network destination.

49. (New) The computer-readable storage device of claim 27, wherein the first data is reconfigured so that only the addresses of the first gateway and the second gateway are available to other users of the network.

50. (New) The computer-readable storage device of claim 30, wherein the security protocol allows only the addresses of the first gateway and the second gateway to be available to other users of the network.

51. (New) The computer-readable storage device of claim 34, wherein the security protocol allows only the addresses of the first gateway and the second gateway to be available to other users of the network.